EE4758 Information Security – Assignment 1

Shoon Zhen Yong (U1920283L)

**Introduction**

Since the prevalence of the COVID-19, we witness a drastic change in the way we live

Ransomware is a type of malware attack in which the attacker locks and encrypts the victim’s data, important files and then demands a payment to unlock and decrypt the data. The earliest variants of ransomware were developed in the late 1980s, and payment was to be sent via snail email. Today, ransomware authors order that payment be sent via cryptocurrency. Most ransom. Most ransomware attacks are triggered by tricking users into clicking on deceptive links using social engineering tactics or by exploiting system vulnerabilities. An attacker always demands payment in cryptocurrency, mainly Bitcoin as taking payments this way reduces the risk of being caught.

**Ransomware Attacks**

The average ransom demand in the first half of 2021 amounted to $5.3 million - a 518% increase compared to 2020. The average ransom payment has also increased by 82% since 2020, reaching a whopping $570,000 in the first half of 2021 alone.

**Common Types of Ransomware Attacks**

1. **Crypto-ransomware**

The goal of crypto ransomware is to hack and [encrypt](https://us.norton.com/internetsecurity-privacy-what-is-encryption.html) the sensitive files located on the victim’s computer, such as documents, pictures, or videos. While cybercriminals withhold access to these files, they don’t go as far as interfering with basic computer functions like other types of ransomware. Hackers want to create a sense of panic within the user by allowing them to see their files without the ability to open their information.

1. **Locker ransomware**

Locker ransomware is unique in that it solely aims to lock victims out of their computers. Hackers do this by disabling all basic computer functions with an exception for minor mouse and keyboard capabilities. Leaving the mouse and keyboard somewhat operable lets the user fulfill the demands of the cybercriminal to gain access back into their device.

A common trend with locker ransomware is that it generally doesn’t target specific files. So, the likelihood of data destruction is lower compared to other types of ransomware attacks. However, there are no guarantees when dealing with cybercriminal masterminds.

1. **Scareware**

[Scareware](https://us.norton.com/internetsecurity-online-scams-how-to-spot-online-scareware-scams.html) is a malicious software created to make false claims about viruses infecting a user's computer or device. A payment is typically requested from the owner to solve the falsified issues. While some types of scareware can lock a user out of their device, others will only go as far as flooding the screen with countless pop-ups to overwhelm the user.

1. **Ransomware as a Service (RaaS)**

Ransomware as a Service (RaaS) is a dark web business model created to help ransomware hackers streamline their attacks. Developers created this software to automatically carry out all aspects of a ransomware attack for the cyberthief, from sending out the ransomware to collecting payments and restoring user access

1. **Doxware or Leakware**

[Doxware](https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html), also known as leakware, threatens the distribution of sensitive data online, targeting people and businesses alike. Since hackers know people, and especially businesses, will do almost anything to prevent confidential and [personal data](https://us.norton.com/internetsecurity-privacy-personal-data-leaking-digital-exhaust.html) from falling into the wrong hands, they often demand compensation to prevent its release.

**Protective Measures Against Ransomware Attacks**

1. Government
2. Public awareness campaigns
3. Information websites
4. Businesses
5. Setting up cybersecurity policies and provide training
6. Phishing stimulation
7. Strengthen cybersecurity technologies
8. Employee education training
9. Individuals

Avoid suspicious links

Create stronger email protections

Improve password security

Keep backups of data and information

**Conclusion**

We must always be mindful to everything around us, including the services we use and the person we engage with. We must be careful when clicking any emails from unknown senders. This is because phishing emails are tailored in the way to make the readers feel nervous or curious. So, we must always remember to first check for the credibility of the source, and not to give personal information and password.

Besides, we must always ensure the safety of our devices. We can install antivirus software to auto-detect malwares in our device. We should not let others to simply take control of our device, be it physical control or remote access. This is risky as it will give attackers chance to steal our data or inject virus into our device.

Moreover, we should always keep ourselves updated to the latest cybersecurity news so that we know what the latest trend of social engineering attacks are, and can be more aware of the risks. We can keep a lookout at the official information released by the national cybersecurity agency, or read about the previous attacks so that we will be less likely to fall into the trap set by the attackers.

**References**

**[1]** https://www.pandasecurity.com/en/mediacenter/security/ransomware-statistics/#:~:text=How%20Common%20Were%20Ransomware%20Attacks,10%25%20of%20all%20data%20breaches.

**[2]**

**[3]**

**[4]**

**[5]**